# Risk Management Framework: Business Case

Gary E. McGraw, Cigital, Inc. [vita[3]]

2005-09-21

The ever-increasing integration of business processes and IT systems means that software risks can often be linked to serious and specific impacts on the mission of an organization or business. Since resources are rarely unlimited, mitigation of software risks can and should be prioritized according to the severity of the related business risks.

Central to the notion of risk management is the idea of clearly describing impact. Without a clear and compelling tie to either business or mission consequences, technical risks, software defects, and the like are not often compelling enough on their own to spur action. The risks we focus on in this portal are all tied directly to software and all have clear security ramifications. However, unless these risks are described in terms that business people and decision makers understand, they will not likely be addressed. The ever-increasing integration of business processes and IT systems means that software risks can often be linked to serious and specific impacts on the mission of an organization or business. Since resources are rarely unlimited, mitigation of software risks can and should be prioritized according to the severity of the related business risks.

All businesses understand the principles and practices of risk management at some level. Executives make use of risk management concepts on a daily basis. Strategic decisions and tactical moves are often informed with risk management data. Business dashboards include business risks as critical measures. Yet software development has not traditionally leveraged this understanding of risk management to gain a clear business mandate. Software security can benefit from a mature risk management framework (RMF) as described here.

Software risk management can only be successfully carried out in a business context. Risks are unavoidable and are a necessary part of software development. Management of risks, including the notion of risk aversion and technical tradeoff, is deeply impacted by business motivation. Thus the first stage of the RMF involves getting a handle on the business situation. Commonly, business goals are neither obvious nor explicitly stated. In some cases, a business may even have difficulty expressing these goals clearly and consistently. When applying the RMF, the analyst must extract and describe business goals, priorities, and circumstances in order to understand what kinds of software risks to care about and which business goals are paramount. Business goals include, but are not limited to, increasing revenue, meeting service level agreements, reducing development costs, and generating high return on investment.

Large numbers of technical risks will be apparent in almost any given system. Identifying these risks is important, but it is the prioritization of these risks that leads directly to creation of value. Through the activities of synthesizing and prioritizing risks, the critical "who cares?" question can (and must) be answered. Ranking of risks is directly related to business impact. Clearly, the risk prioritization process must take into account which business goals are the most important to the organization, which goals are immediately threatened, and how likely technical risks are to manifest themselves in such a way as to impact the business.

The essential business activities of identifying, tracking, storing, measuring, and reporting software risk information cannot be overemphasized. Successful use of the RMF depends on continuous and consistent identification and storage of risk information as it changes over time. A master list of risks should be maintained during all stages of RMF execution and continually revisited. Measurements regarding this master list make excellent reporting fodder. For example, the number of risks identified in various software artifacts and/or software life-cycle phases can be used to identify problematic areas in software process. Likewise, the number of software risks mitigated over time can be used to show concrete progress as risk mitigation activities unfold. Links to descriptions or measurements of the corresponding business risks

[3] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/198-BSI.html (McGraw, Gary)

mitigated can be used to clearly demonstrate the business value of the software risk mitigation process and the risk management framework.

## Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com